UNITED STATES DISTRICT COURT
SOUTHERN DISTRICT OF NEW YORK

UNITED STATES OF AMERICA	:	
- v. -	:	21 Cr. 536 (JSR)
JOSEPH JAMES O'CONNOR, a/k/a "PlugwalkJoe,"	:	23 Cr. 225 (JSR)
Defendant.	:	

GOVERNMENT'S SENTENCING MEMORANDUM
REGARDING DEFENDANT JOSEPH JAMES O'CONNOR

DAMIAN WILLIAMS
United States Attorney
Southern District of New York
Attorney for the United States of America

Olga I. Zverovich
Assistant U.S. Attorney
(Of Counsel)

KENNETH A. POLITE, JR.
Assistant Attorney General
Criminal Division
U.S. Department of Justice

Adrienne L. Rose
Assistant Deputy Chief
Computer Crime and Intellectual Property Section

TABLE OF CONTENTS

UNITED STATES DISTRICT COURT
SOUTHERN DISTRICT OF NEW YORK

- -x

UNITED STATES OF AMERICA	:	
- v. -	:	
	:	21 Cr. 536 (JSR) 23 Cr. 225 (JSR)
JOSEPH JAMES O'CONNOR, a/k/a "PlugwalkJoe,"	:	
Defendant.	:	

- -x

GOVERNMENT'S SENTENCING MEMORANDUM
REGARDING DEFENDANT JOSEPH JAMES O'CONNOR

PRELIMINARY STATEMENT

The Government respectfully submits this memorandum in advance of the sentencing of defendant Joseph James O'Connor, which is scheduled for June 23, 2023.

As described in detail below, between March 2019 and August 2020, O'Connor went on a spree of destructive and disturbing criminal conduct targeting a broad range of victims. O'Connor perpetrated cyber intrusions targeting U.S. companies, stealing a large amount of cryptocurrency from one of them. O'Connor defrauded, threatened, abused, and extorted several individual victims, including a 16-year-old girl against whom O'Connor perpetrated vicious swatting attacks, prompting an emergency police response. O'Connor's crimes caused substantial financial and emotional harm to his victims.

To reflect the seriousness of the defendant's conduct, to provide just punishment and promote respect for the law, and to deter the defendant and others like him, the Government respectfully requests that the Court impose a sentence of seven years' imprisonment, which would be sufficient but not greater than necessary to serve the legitimate purposes of sentencing.

FACTUAL BACKGROUND

I. Offense Conduct

O'Connor stands to be sentenced for his convictions on two separate sets of charges, which were originally filed in the Southern District of New York (the "SDNY Case") and the Northern District of California (the "NDCA Case"). O'Connor's conduct in each case is discussed in turn below.

A. SDNY Case

From about March 2019 to May 2019, O'Connor, working together with other co-conspirators, perpetrated a SIM swap scheme,[1] which involved the theft of a large amount of cryptocurrency, then valued at approximately $794,000 (and currently valued at more than $1.4 million), belonging to customers of a victim company ("Company-1"), a technology company headquartered in Manhattan that provides wallet infrastructure and related software to cryptocurrency exchanges around the world. As described in detail below, after stealing the cryptocurrency, O'Connor and his co-conspirators laundered it through dozens of transfers and transactions, with some of it ultimately transferred into a cryptocurrency exchange account controlled by O'Connor.

[1] A "SIM card" is a subscriber identity module or subscriber identification module. A cellphone requires a SIM card to connect the cellphone to a mobile phone network. The SIM card in a particular cellphone is generally linked to the phone number for that cellphone. In general terms, a SIM swap scheme occurs when a scheme participant causes a phone carrier to switch a victim's phone number over to a SIM card that the scheme participant or a co-conspirator controls. By doing so, the scheme participant is able to receive messages intended for the victim, which the scheme participant may then use to, among other things, reset passwords on, and access, accounts held by the victim, such as email and bank accounts. (Presentence Investigation Report ("PSR") ¶ 22).

The SIM Swap Attacks Against Executive-1

Company-1's co-founder and Vice President of Development ("Executive-1") was the victim of SIM swap attacks in March and late April 2019. As described below, the SIM swap attack against Executive-1 in late April 2019, perpetrated by O'Connor and his co-conspirators, resulted in the successful theft of a large amount of cryptocurrency from Company-1. (PSR ¶ 24).

AT&T records for Executive-1's mobile account show that two different malicious unauthorized devices, identified by IMEI numbers[2] 355396080751723 ("Malicious Device-1") and 990002825675752 ("Malicious Device-2"), were associated with Executive-1's mobile account on April 30, 2019. Based on AT&T records, the suspected malicious devices remained associated with Executive-1's mobile account for approximately three hours. (PSR ¶ 25).

O'Connor's co-conspirators in the United States ("CC-1" and "CC-2"), both of whom were minors at the time of the SIM swap attack, physically held the malicious devices (Malicious Device-1 and Malicious Device-2) that were fraudulently linked to Executive-1's mobile account as part of the SIM swap attack. Both CC-1 and CC-2 perpetrated SIM swap attacks with O'Connor, including the SIM swap attack against Executive-1. (PSR ¶ 26).

O'Connor's and His Co-Conspirators' Intrusions into Company-1's Computer Systems and Theft of Cryptocurrency

Approximately one hour after the April 2019 SIM swap attack perpetrated by O'Connor and his co-conspirators against Executive-1, several accounts in Company-1's G Suite,[3] including the Administrator account, were subject to unauthorized access. (PSR ¶ 28).

[2] An International Mobile Equipment Identity ("IMEI") number is a 15-digit number that uniquely identifies a particular mobile device. (PSR ¶ 25 n.2).

[3] G Suite is a collection of tools, software, and products offered by Google. (PSR ¶ 28 n.3).

Over approximately the next three days, multiple Company-1 servers and its Microsoft Azure environment[4] were subject to unauthorized access. As part of the attack, O'Connor and his co-conspirators changed the passwords on, and used employees' account login credentials without authorization to log in to, the G Suite accounts used by several Company-1 employees, including employees in Company-1's Manhattan office. (PSR ¶ 29).

As part of the attack, on May 1, 2019, O'Connor and his co-conspirators stole and withdrew cryptocurrency of various types, which belonged to two clients of Company-1, from cryptocurrency wallets on the compromised servers. The cryptocurrency, valued at approximately $794,000 at the time (and currently valued at more than $1.4 million), was stolen through the attack as follows (the "Stolen Cryptocurrency"):

Coin Type	Amount	Timestamp (UTC)	Affected Customer
Bitcoin Cash	770.784869	5/1/19 01:17:00	Customer-1
Litecoin	6363.490509	5/1/19 01:18:39	Customer-1
Ethereum	407.396074	5/1/19 01:19:36	Customer-2
Bitcoin	7.456728	5/1/19 01:23:18	Customer-1

(PSR ¶ 30; *see also* PSR ¶¶ 89-90).

In the days after the theft, two other Company-1 executives ("Executive-2" and "Executive-3") were victims of SIM swap attacks. On May 4, 2019, following these attacks, one of the conspirators accessed Executive-2's Skype account without authorization and used it to start an online group chat with Company-1 employees, which continued for about two hours. During the Skype chat, the attacker referenced the SIM swap attack against Executive-1, the unauthorized

[4] Microsoft Azure is a cloud computing-based service similar to Google cloud platform. (PSR ¶ 29 n.5).

access to Company-1's computer systems, and the theft of cryptocurrency from Company-1's wallets. The attacker also taunted Company-1 employees about "[g]etting hacked by a group of kids." (PSR ¶ 31).

Laundering of the Stolen Cryptocurrency

After stealing the cryptocurrency from Company-1, O'Connor and his co-conspirators laundered it through dozens of transfers and transactions, and some of it was exchanged for bitcoin ("BTC") using cryptocurrency exchange services. (PSR ¶¶ 33-34). O'Connor and his co-conspirators used sophisticated laundering techniques, including the use of mixers and tumblers, as a result of which law enforcement could only trace a subset of the Stolen Cryptocurrency. (PSR ¶ 34 & nn.6-7).

O'Connor controlled three accounts at the cryptocurrency exchange Binance, which were closely connected to the attack against Company-1, including through a common malicious internet protocol ("IP") address that was used to access both Company-1's G Suite accounts during the cyber intrusion and O'Connor's Binance accounts. One of O'Connor's Binance accounts received a portion of the laundered Stolen Cryptocurrency. (PSR ¶¶ 35-37).

O'Connor's crimes caused substantial economic and non-economic harm to Company-1 and its employees. (PSR ¶ 88). Company-1's counsel has submitted a victim impact statement to this Court, which is attached hereto as Exhibit A.[5]

[5] Company-1 is concerned about preserving its anonymity and has, through counsel, requested that the victim impact statement be filed under seal.

Relevant Conduct: Account Takeovers

In addition to participating in the cyber intrusion against Company-1, O'Connor was also involved in the following account takeovers[6] involving three individual victims on May 12 and 15, 2019, *i.e.*, shortly after the Company-1 intrusion:

- A Coinbase account of a victim ("SDNY Individual Victim-1") was compromised on May 12, 2019, and approximately 0.5 BTC were stolen. On the same day, SDNY Individual Victim-1's Gemini account was compromised, and approximately 0.02 BTC were stolen.

- A Gemini account of a second victim ("SDNY Individual Victim-2") was compromised on May 12, 2019, the same date as the compromises of SDNY Individual Victim-1's accounts described above, and approximately 1.67 BTC were stolen.

- A Coinbase account of a third victim ("SDNY Individual Victim-3") was compromised on May 15, 2019, and approximately 18.03 BTC were stolen.

(PSR ¶¶ 38-39).

B. NDCA Case

The Twitter Hack

On July 15, 2020, O'Connor, along with co-coconspirators, engaged in a large-scale and widely publicized computer intrusion into Twitter, Inc. ("Twitter"), resulting in the unauthorized access of approximately 130 accounts. During the attack, Twitter detected a coordinated social engineering effort targeting its employees with access to internal systems and tools. As a result of this attack, numerous high-profile individuals' accounts were compromised, including those belonging to elected officials, including then-former Vice President Joseph Biden and former

[6] In an account takeover, a malicious cyber actor gains unauthorized access to a victim's online account and uses that access to conduct unauthorized activities within the account. In the case of a cryptocurrency exchange account, the online actor typically utilizes the account to buy, exchange, deposit, and/or withdraw cryptocurrency. In many cases when the victim has a balance of cryptocurrency stored in the account or has linked fiat banking services to the account (*e.g.* debit card, ACH transfer), the cyber actor can steal funds from the account. (PSR ¶ 38 n.9).

President Barack Obama; business leaders, including Bill Gates and Elon Musk; celebrities, including Kanye West; and companies, including Apple and Uber. (PSR ¶¶ 41-42, 45).

O'Connor's co-conspirator ("Juvenile-1") exploited this unauthorized access by monetizing the transfer of Twitter accounts from their rightful accountholders to various unauthorized users. Co-conspirators who took control of the accounts in turn launched a scheme to defraud other Twitter users. For example, one co-conspirator took over Elon Musk's Twitter account and posted: "I'm feeling generous because of Covid-19. I'll double any BTC [bitcoin] payment sent to my BTC address for the next hour. Good luck, and stay safe out there!" In the post, the co-conspirator provided a bitcoin address, purportedly belonging to Elon Musk, in an effort to fraudulently obtain bitcoin from Twitter users. (PSR ¶¶ 43-45).

During the course of the Twitter hack, O'Connor communicated with Juvenile-1 and other co-conspirators about obtaining access to specified accounts, including accounts associated with public figures. O'Connor also used his Twitter account to view accounts involved in the hack in order to determine if such accounts were suspended or active, which would enable them to be compromised. A number of accounts targeted by O'Connor were subsequently transferred away from their rightful owners. (PSR ¶¶ 48, 50-51).

For example, on July 15, 2020, O'Connor used his Twitter account to view at least ten accounts that were subsequently accessed or taken over during the Twitter hack. O'Connor also communicated with a co-conspirator who served as a middleman for Juvenile-1 about the cost of access to Twitter accounts "@6," "@lost," "@y," "@alone," and "@vampire," among others. After the co-conspirator informed Juvenile-1 of O'Connor's interest in the accounts, including that O'Connor offered to pay $10,000 for the "@6" Twitter account, Juvenile-1 changed the display

name to O'Connor's alias, "pwj," and the account avatar to an image requested by O'Connor. (PSR ¶¶ 49, 51).

During the Twitter hack, O'Connor publicly posted messages on Twitter sharing his and his co-conspirators' access to Twitter's administrative tools. On July 15, 2020, O'Connor posted a public message on his Twitter account "@shinji"[7] with images of Twitter's internal administrative tool accessing an account, with the message, "twitter admin tools be like":

[7] Authorities have determined that the Twitter account "@shinji" was operated by O'Connor. The user of the "@shinji" account stated that the account replaced his "@PlugwalkJoe" account and referred to himself as "PlugwalkJoe" and "joseph." The same IP addresses were used to access the "@shinji" account that accessed O'Connor's Snapchat account, "j.oconnor99" (which was used in the commission of the offenses against Victim-2), Instagram account "j0e" (which was used in the commission of the offenses against Victim-2 and Victim-3), and a Discord account (which was used in the commission of the Twitter hack). Further, the "j.oconnor99" Snapchat account and "@PlugwalkJoe" Twitter accounts were used to post passport images of O'Connor containing his name, passport number, date of birth, place of birth, and childhood photograph.

Hacking of Victim-1's TikTok Account

Between August 14 and 15, 2020, O'Connor, along with a co-conspirator, engaged in a widely publicized hack of a TikTok[8] account belonging to a social media personality ("Victim-1"), changing the username to "joeandzak1" and updating the biography section to "plugwalkjoe zak n crippin." At the time of this hack, Victim-1 was 19 years old and her TikTok account—with over 55 million followers—was one of the most viewed and followed accounts on TikTok. (*See* PSR ¶¶ 53-54).

In the weeks leading up to the hack of Victim-1's TikTok account, O'Connor communicated with co-conspirators regarding Victim-1. On August 6, 2020, a co-conspirator provided O'Connor with Victim-1's phone number, cellular provider, and the names of Victim-1's parents. The co-conspirator asked O'Connor to promote the co-conspirator's Twitter account if O'Connor was successful at taking over Victim-1's TikTok account. (PSR ¶ 55).

On August 14, 2020, O'Connor sent to the co-conspirator a screenshot of Victim-1's TikTok account, demonstrating that he was logged into the account. Shortly thereafter, O'Connor began posting videos on Victim-1's TikTok account. (PSR ¶ 56).

During the attack, O'Connor posted multiple videos to Victim-1's TikTok account promoting O'Connor's own social media accounts and his alias "Plug Walk Joe." He also posted videos offering to share nude images of Victim-1. For example, in one video posted on August 15, 2020, O'Connor provided links to Discord chats,[9] with a message stating, "Join these discords

[8] TikTok is a video-sharing social networking service that is used to create short videos that can be shared or stored publicly or privately. TikTok allows users to interact with each other through comments to videos, direct messages, and live chats. (PSR ¶ 52).

[9] Discord is a social media platform that offers chat channels where users can communicate via text messages, voice, and video. (PSR ¶ 47 n.3).

for [Victim-1] nudes #plugwalkwashere." O'Connor spoke in the background of the video stating, "Yo, join these servers man. Plug walk." (PSR ¶ 57).

In another video posted to Victim-1's TikTok account on August 15, 2020, O'Connor promoted his co-conspirator's Twitter account. O'Connor spoke in the background of the video stating, "Yo. Shout out to my boy Cal on Park Lane, for real. Follow @speaker on Twitter. I'll give you [Victim-1's] number or nudes. Whatever you want, bro." (PSR ¶ 58).

Hacking of Victim-2's Snapchat Account and
Cyberthreats and Extortion of Victim-2

Between June 13 and 15, 2019, O'Connor, along with a co-conspirator, engaged in a widely publicized takeover of a Snapchat[10] account belonging to a 21-year-old victim ("Victim-2"). As part of the attack, O'Connor stole and disseminated Victim-2's sensitive nude photographs and videos from the account to his associates, and engaged in an extortion campaign threatening to release the images publicly if Victim-2 did not promote O'Connor and his co-conspirators. To avoid being extorted, Victim-2 ultimately released the nude photographs herself. (PSR ¶ 60).

On June 13, 2019, O'Connor and co-conspirators engaged in a SIM swap on Victim-2's cell phone, enabling O'Connor to gain unauthorized access to Victim-2's Snapchat account. O'Connor captured a screen recording of his iPhone as he gained access to Victim-2's account, which he shared with friends. (PSR ¶¶ 60-63).

After gaining unauthorized access to Victim-2's Snapchat account, O'Connor sent numerous nude photographs and videos of Victim-2 to his associates. O'Connor also posted messages on Victim-2's account promoting O'Connor's own social media accounts and offering to share nude images of Victim-2 if O'Connor's social media accounts received a certain threshold

[10] Snapchat is a popular application for sending and receiving "self-destructing" messages, pictures, and videos. (PSR ¶ 59).

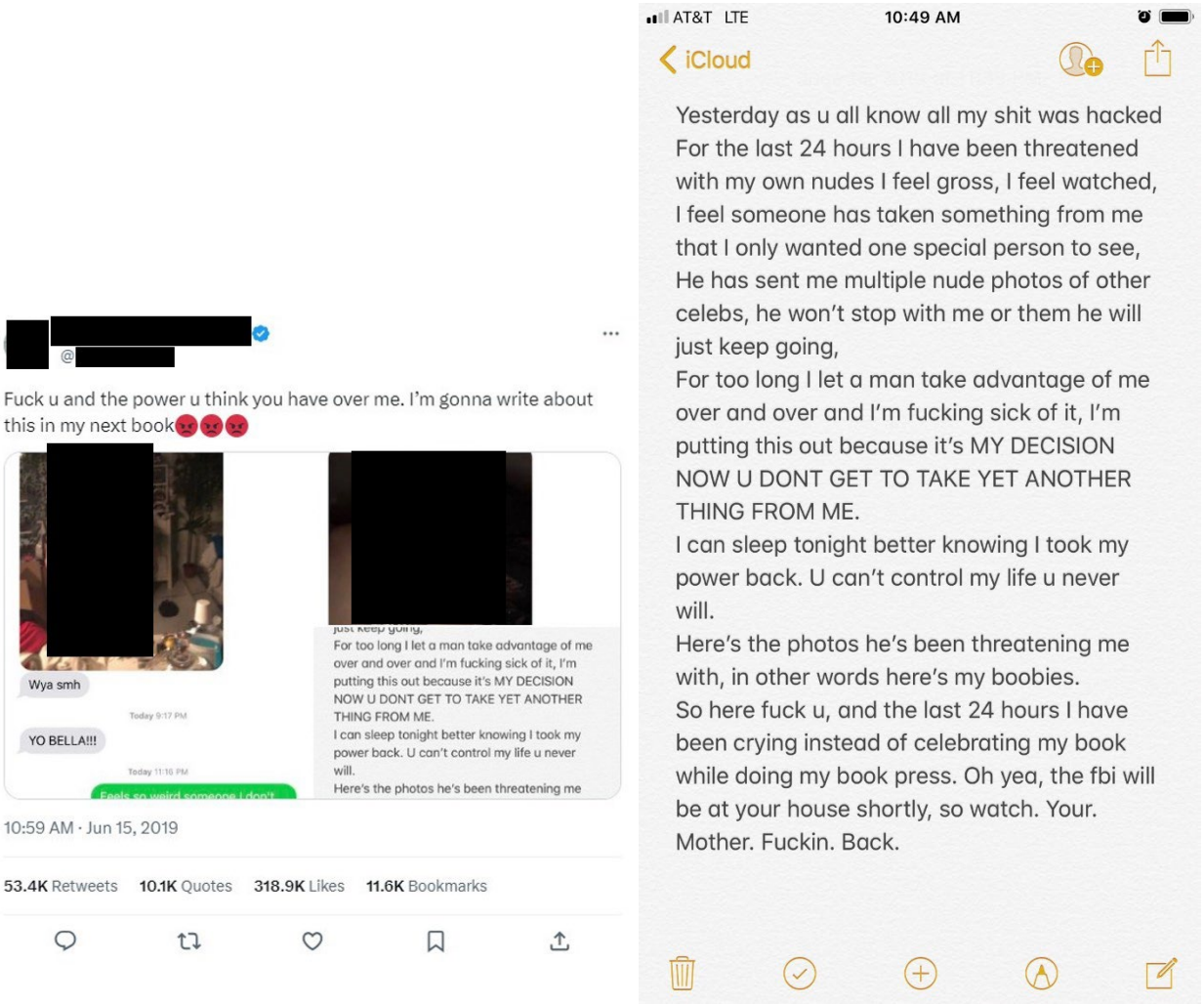
of followers. For example, O'Connor posted a message on Victim-2's Snapchat account stating that viewers should "Add j.oconnor99 on Snapchat for [Victim-2] nudes he's dropping them on story at 20 k adds." In another post, O'Connor stated, "Will drop nudes if 5000 of you follow @PlugwalkJoe." O'Connor's Snapchat account received numerous chat messages from people asking about "[Victim-2's] nudes" and similar content. (PSR ¶¶ 64-66).

On June 14, 2019, O'Connor sent an associate nine photographs and four videos of Victim-2, all of which depicted Victim-2 nude. That associate subsequently sent text messages to Victim-2 directing Victim-2 to post a tweet promoting O'Connor's and others' social media accounts. The associate sent a screenshot of these extortionate text messages to O'Connor. In the screenshot, Victim-2 stated, "Feels so weird someone I don't know looking at my personal shit." The associate responded, "listen Do the tweet n we good? It'll be the entire internet looking at your personal shit.. just do my tweet." (PSR ¶¶ 64, 67-68).

Victim-2 provided law enforcement with screenshots of the text message conversation. Victim-2 reported that on June 14, 2019, she received a text message that stated, "yo [Victim-2] this is the hacker from yday I got your nudes from yday but I won't show anyone or leak them if you just tweet out like 'I was hacked yesterday, thanks to the hackers @MyUsername for giving me my accounts back.'" The associate later stated, "the tweet would be this 'I was hacked yesterday, thanks to @NuBLoM, Debug and PlugwalkJoe for giving me my accounts back.'" After Victim-2 asked for proof that the associate had nude images of her, the associate responded with the nine photographs that O'Connor had had obtained from Victim-2's Snapchat account and sent to the associate earlier. (PSR ¶¶ 69-70).

On June 15, 2019, to avoid being extorted, Victim-2 posted the nude images of herself on Twitter, explaining, "For the last 24 hours I have been threatened with my own nudes. . . . I'm

putting this out because it's MY DECISION[,] NOW U DON'T GET TO TAKE YET ANOTHER THING FROM ME":



(PSR ¶ 71).

Following O'Connor's arrest, Victim-2 made an additional public statement about the incident on Instagram, describing O'Connor as "the person who made my life and others a living hell":

49,751 likes

[redacted] I want to thank the FBI for searching tirelessly for the person who made my life and others a living hell. I have felt violated many times in my life, but I thought I didn't have a way out, so I made a choice. My choice. A choice I didn't want to make but felt I had to because I wouldn't spend another day feeling someone was taking away from me my body, my soul, my mental health, and my love and hope for the world. So thank you, FBI, for a step in the right direction and just one less bad guy to worry about. Today I woke up with hope again, and a weight lifted off my shoulders. But with that said, I still need to get something across that I have wanted to say for a long time. For all the people who think because a woman is comfortable with their body and how they portray themselves that they are "asking for it, "for the people who think "she deserves it" because she was there or had a beer in her hand or wore a short skirt, and for the people that think because she took the photo she deserves to be humiliated with it - and she deserves for everyone to look at it and inscribe every piece and bit of her in their mind.Or because she took the photo, she deserves that one moment to follow her, taunt her for the rest of her life through every waking moment.To those who made those remarks, they were disgusting. I hope you feel disgusting.To those few people.
Sincerely [redacted] you.

Cyberthreats and Swatting of Victim-3

In June and July 2020, O'Connor orchestrated a campaign of cyberthreats, harassment, and swatting attacks[11] against a 16-year-old victim ("Victim-3") and her family members. (PSR ¶ 72).

O'Connor met Victim-3 online in a chatroom on the Discord social media platform. Over the first few days of the chats, O'Connor sent Victim-3 numerous inappropriate messages, including that he would kill her and fuck her dead body. O'Connor also sent Victim-3 a photograph of his penis, including comments such as ". . . fuck your mouth and cum down into your stomach." Prior to receiving this photograph, Victim-3 told O'Connor that she was 16 years old. (PSR ¶ 82).

On June 24, 2020, the day before the swatting incidents, O'Connor told Victim-3 to "keep my name our [sic] ur mouth." (PSR ¶ 86). Starting June 25, 2020, four days after meeting Victim-3, O'Connor perpetrated a series of swatting attacks against Victim-3. (PSR ¶¶ 74-81).

In the first series of swatting incidents, O'Connor posted on a Reddit web forum that an individual identified as Victim-3 was making threats to shoot at minorities in Garden Grove, California. The Reddit post gave an address for anyone who had guns and wanted to be part of the shooting to meet at a specified address, which O'Connor had thought was Victim-3's home and which was in fact Victim 3's neighbor's house. O'Connor then reported that Reddit post to the Garden Grove Police Department. (PSR ¶ 74).

A few hours later, O'Connor contacted the same police department and falsely reported that he had caught his wife, whom he identified as Victim-3, cheating and that he planned to kill her and his six children unless he received $50,000. O'Connor threatened to kill any law

[11] A "swatting" attack occurs when an individual makes a false emergency call to a public authority in order to cause a law enforcement response that may put the victim or others in danger. (PSR ¶ 73).

enforcement officer responding to the scene. O'Connor stated that his children were black and he wanted to kill them because "black lives don't matter." He said that he could not find his bomb but had a Molotov cocktail. He gave the same address that he believed to be Victim-3's home. (PSR ¶ 75).

As a result of O'Connor's actions, the Garden Grove Police Department dispatched every on-duty officer and two sergeants to respond to that address. During the course of that significant police response, O'Connor reported to the Orange County Sheriff's Department that he was at that address and was going to kill his wife and children. O'Connor also reported to Orange County Fire Authority that the same address was on fire. (PSR ¶¶ 76-77).

O'Connor perpetrated a second set of swatting attacks against Victim-3 on the same day, June 25, 2020. O'Connor sent an email to Victim-3's high school principal, identifying himself as Victim-3 and threatening the school district with shootings and bombings:[12]

> My name is [Victim-3]. I will be shooting up schools in Garn Grove, California at random times on Tuesday. . . I will be aiming at minority students (Black, Mexican, Asian, Etc) As they need to get the fuck off American soil and give us our freedom back!! All those niggers do is rob and steal! . . . I also snuck in over the weekend and put pipe bombs and duffel bags with bombs in them.

(PSR ¶ 78).

In a third series of swatting incidents targeting Victim-3 on the same day, O'Connor made a series of posts relating to attacks at restaurants by Victim-3. For example, O'Connor posted the following statement on Reddit:

---

[12] The email was sent from "markwoodjhonson02@gmail.com" from an IP address that was associated with three other accounts (Discord, Reddit, and Google) associated with O'Connor. The phone number registered to the "markwoodjhonson02@gmail.com" email was the number used to call the Garden Grove Police Department threatening use of a Molotov cocktail, in the first set of swatting incidents, and to call the Orange County Sheriff's Department with a bomb threat at the airport, in the fourth set of swatting incidents, described below.

> Hello, my name is [Victim-3]. I will be shooting at people in Garn Drove, California at random times on Tuesday . . . I will be aiming at minorities (Black, Mexican, Asian, Etc) As they need to get the fuck off American soil and give us our freedom back!! Also those niggzzz do is rob and steal! . . . I've planted pipe bombs in the Joes Crab Shack . . . and at Coco's Bakery Restaurant."

(PSR ¶ 79).

In the final set of swatting attacks on Victim-3 that day, O'Connor made a bomb threat against an airport. O'Connor contacted the Orange County Sheriff's Department, identified himself as Victim-3, and stated that he (Victim-3) was "a transgender going to blow up the airport in 24 hours." He requested $60,000 or else he would kill everyone at the airport. O'Connor directed that the money be sent to the address that he believed to be Victim-3's residence. O'Connor subsequently called again, provided the same address, and stated, "I have an AR-15 with a silencer and I just killed my wife. I told you guys to come." (PSR ¶¶ 80-81).

O'Connor's victimization of Victim-3 did not end there. In another series of cyberattacks on Victim-3, starting on July 16, 2020, O'Connor began calling several of Victim-3's relatives. In each call, O'Connor threatened Victim-3's relative. (PSR ¶ 83).

On July 25, 2020, Victim-3 spoke with O'Connor over FaceTime. O'Connor apologized for his actions but said that she had deserved it. Despite Victim-3 again telling O'Connor that she was 16, O'Connor continued to make comments of a sexual nature toward her. (PSR ¶ 84).

Over the course of his contact with Victim-3, which continued from June 20, 2020, to August 22, 2020, O'Connor recorded multiple communications that he had with Victim-3 over his Snapchat account. In one recording from July 25, 2020, O'Connor stated to Victim-3, "I doxed you and called your mom. . . I doxed you. Is that fucked up?" In another recording, O'Connor claimed he did not call the police. (PSR ¶¶ 85-86).

O'Connor's criminal conduct caused substantial emotional distress to Victim-3. (PSR ¶ 87).

II. Procedural History

On May 14, 2021, O'Connor, a U.K. citizen, was charged by Complaint (3:21-mj-70812 MAG) (the "NDCA Complaint") in the Northern District of California.

On July 21, 2021, O'Connor was arrested in Spain on the charges in the NDCA Complaint, and extradition proceedings related to the NDCA Complaint ensued. O'Connor was detained in Spain pending the extradition proceedings.

On August 25, 2021, a four-count Indictment, 21 Cr. 536 (the "SDNY Indictment"), was filed under seal in this District, charging O'Connor with conspiracy to commit computer intrusions, in violation of 18 U.S.C. § 371 (Count One); conspiracy to commit wire fraud, in violation of 18 U.S.C. § 1349 (Count Two); aggravated identity theft, in violation of 18 U.S.C. §§ 1028A(a)(1)&(b) and 2 (Count Three); and conspiracy to commit money laundering, in violation of 18 U.S.C. § 1956(h) (Count Four).

In or about September 2021, the Government submitted an additional extradition request based on the SDNY Indictment to Spain, where O'Connor was already in extradition proceedings pursuant to the NDCA Complaint. The SDNY Indictment was unsealed on November 2, 2021.

While O'Connor's extradition proceedings were pending in Spain, the parties negotiated a plea resolution by which O'Connor would resolve both the SDNY and the NDCA charges against him through a guilty plea in this District.

In late March 2023, the Government was advised that O'Connor has been ordered extradited from Spain to the United States on the charges in the SDNY Indictment and the NDCA Complaint.

On April 18, 2023, a seven-count criminal Information, 23 Cr. 113 (RS), was filed in the Northern District of California (the "NDCA Information"). The charges in the NDCA Information are based on the same conduct alleged in the NDCA Complaint.

On April 26, 2023, O'Connor was surrendered to the United States. On April 27, 2023, O'Connor was presented and arraigned before this Court on the charges in the SDNY Indictment. O'Connor was detained.

On May 4, 2023, the NDCA Information against O'Connor was transferred to this District pursuant to Federal Rule of Criminal Procedure 20. The case was ultimately assigned to this Court under docket number 23 Cr. 225 (JSR).

On May 9, 2023, O'Connor was arraigned on the charges in the NDCA Information and pleaded guilty before this Court to Counts One, Two, and Four of the SDNY Indictment and Counts One through Seven of the NDCA Information.

U.S. SENTENCING GUIDELINES CALCULATION

The parties agree that O'Connor's Guidelines range is 70 to 87 months' imprisonment, based on a total offense level of 27 and a Criminal History Category of I. (PSR ¶ 17). The Guidelines range as calculated by the U.S. Probation Office in the Presentence Report is the same as that set forth in the parties' plea agreement. (PSR ¶¶ 102-57, 210). Although the Presentence Report attributes four additional offense levels to one of the groups of offenses, namely Group 3, as compared with the plea agreement (*compare* PSR ¶ 17(A)(14)-(19), *with* PSR ¶¶ 125-31), this difference does not impact O'Connor's Guidelines range.

Notably, the Guidelines range is driven almost entirely by the SDNY Case. Notwithstanding the seriousness of O'Connor's criminal conduct in the NDCA Case, the NDCA Case results only in a one-level increase to O'Connor's offense level. (PSR ¶¶ 146-49).

The Probation Office recommends a sentence of 70 months' imprisonment. As the Probation Office explains, "we have reviewed all the factors available to us in this case and found nothing that can overcome the seriousness of the conduct": "[t]he defendant caused a tremendous amount of financial, and emotional harm," including through swatting attacks that "were egregious and caused extreme disruption." (PSR at 50).

ARGUMENT

I. A Sentence of Seven Years' Imprisonment is Necessary to Satisfy the Purposes of Sentencing

A. Applicable Law

As the Supreme Court stated, "a district court should begin all sentencing proceedings by correctly calculating the applicable Guidelines range"—that "should be the starting point and the initial benchmark." *Gall v. United States*, 552 U.S. 38, 49 (2007).[13]

After calculating the Guidelines range, a sentencing judge must consider the factors set forth in Section 3553(a) and "impose a sentence sufficient, but not greater than necessary, to comply with the purposes" of sentencing: "a) the need to reflect the seriousness of the offense, to promote respect for the law, and to provide just punishment for that offense; b) the need to afford adequate deterrence to criminal conduct; c) the need to protect the public from further crimes by the defendant; and d) the need for rehabilitation." *United States v. Cavera*, 550 F.3d 180, 188 (2d Cir. 2008) (citing 18 U.S.C. § 3553(a)(2)). Section 3553(a) further directs the Court "in determining the particular sentence to impose" to consider: (1) the nature and circumstances of the offense and the history and characteristics of the defendant; (2) the statutory purposes noted above; (3) the kinds of sentences available; (4) the kinds of sentence and the sentencing range as set forth

[13] Unless otherwise noted, case quotations omit all internal citations, quotation marks, and previous alterations.

in the Sentencing Guidelines; (5) the Sentencing Guidelines policy statements; (6) the need to avoid unwarranted sentencing disparities; and (7) the need to provide restitution to any victims of the offense. *See* 18 U.S.C. § 3553(a).

B. Discussion

The Government respectfully submits that a sentence of seven years' imprisonment is necessary to reflect the seriousness and gravity of O'Connor's offense conduct, provide just punishment, afford specific and general deterrence, promote respect for the law, and protect the public from further crimes by O'Connor.

1. The Nature and Circumstances of the Offense and the Need to Provide Just Punishment

O'Connor's crimes are extremely serious and destructive and require commensurate punishment. Over the course of nearly 1.5 years, O'Connor perpetrated a wide variety of cyber-attacks to defraud, threaten, abuse, and extort his victims. In the spring of 2019, O'Connor and his co-conspirators perpetrated SIM swap attacks against Company-1 and stole a large amount of cryptocurrency—currently valued at over $1.4 million—from Company-1 and its clients. O'Connor and his co-conspirators then laundered the proceeds of their cyber intrusion through a web of complex and sophisticated transactions that left law enforcement unable to effectively trace and recover the stolen cryptocurrency. As a result of O'Connor's criminal actions, Company-1 suffered significant harm, both economic and non-economic, and, to date, has not been able to recoup its losses. O'Connor's financial crimes did not end with Company-1. In May 2019, shortly after victimizing Company-1, O'Connor victimized three individuals by taking over their cryptocurrency accounts and stealing their bitcoin.

O'Connor's crime spree was not confined to fraud and financial crimes. O'Connor also reached across the globe to terrorize a variety of vulnerable victims, without any direct financial

incentive, simply to promote his online persona and to show that he had the power to do so. His crimes triggered extreme emotional distress in his victims and put others at risk of physical harm. In June 2019, O'Connor targeted Victim-2 by gaining unauthorized access to Victim-2's Snapchat account through another SIM swap attack. O'Connor obtained nude photographs of Victim-2, disseminated those photographs to others, and, through an associate, tried to extort Victim-2, threatening to release Victim-2's photographs unless Victim-2 promoted O'Connor and his co-conspirators. To avoid being extorted, Victim-2 published the nude photographs herself. Victim-2's public statements regarding the attack reflect the destabilizing horror that O'Connor was able to inflict on his victims. (PSR ¶ 71).

Between June and August 2020, O'Connor moved on to other victims, both corporate and individual. He victimized many others through his participation in the Twitter hack, his hacking into Victim-1's TikTok account, and his repeated and reckless attacks targeting Victim-3. O'Connor's criminal actions toward Victim-3, who was only 16 years old at the time, were particularly disturbing and egregious. O'Connor sent Victim-3 graphic sexual messages, threatened Victim-3's relatives, and engaged in a campaign of vile and vicious swatting attacks against Victim-3. Pretending to be or referencing Victim-3, O'Connor contacted police departments, a fire department, and others, threatening to perpetrate mass shootings, to commit murders, and to bomb an airport, a high school, and restaurants. O'Connor's criminal actions not only caused substantial emotional distress to Victim-3, but they also prompted a significant law enforcement response, taking away much needed law enforcement resources from addressing real emergencies.

O'Connor's crimes, which targeted numerous U.S. victims from behind a computer screen overseas, were extremely serious and inflicted wide-ranging harms on many. The sentence

imposed upon O'Connor must reflect the gravity and seriousness of his criminal conduct and provide just punishment to O'Connor.

The Government respectfully submits that, unlike in some cases, where the loss amount calculation, and consequently the Guidelines range, may overstate the seriousness of a defendant's criminal conduct, the Guidelines range in this case fails to reflect the severe harm that O'Connor inflicted on his victims through his criminal conduct. While the Guidelines range takes into account the financial loss in this case, O'Connor's criminal conduct also caused emotional and psychological harm to his victims—a fact that is not captured by the Guidelines at all. Moreover, O'Connor stands to be sentenced for his criminal conduct in two separate cases, brought independently in two different districts. And yet, because of the operation of the Guidelines, the entirety of O'Connor's extensive criminal conduct in the NDCA Case—which, as this Court observed at O'Connor's arraignment, itself may call "for meaningful prison time" (Arraignment Tr. 15:2, Dkt. No. 8, 21 Cr. 536 (JSR))—results in only one additional Guidelines offense level. Moreover, the one additional offense level stems only from O'Connor's participation in the Twitter hack; his egregious and destructive crimes against Victims-1 through -3 in the NDCA Case are not reflected in the Guidelines calculation at all. The Government respectfully submits that this Court should consider these facts as it evaluates the appropriate sentence under the Section 3553(a) factors.

2. History and Characteristics of the Defendant and the Need to Provide Specific Deterrence and Protect the Public from Further Crimes

The need to afford specific deterrence and protect the public from further crimes by O'Connor further require a significant sentence in this case. Although O'Connor is only 24 years old and is in Criminal History Category I, the facts of this case show that he has committed numerous cybercrimes, targeting a broad range of victims, over the course of his life. In fact,

O'Connor's pattern of destructive cybercrimes predates his conduct in this case, which itself spanned nearly 1.5 years. As O'Connor's mother reported, he was expelled from school for hacking his school's network. (PSR ¶ 176). It is clear that O'Connor's actions were not simply an isolated lapse of judgment made in a moment of weakness. Rather, instead of applying his sophisticated computer skills to improve society and make an honest living, O'Connor has made a conscious decision to live his life by defrauding and victimizing others—individuals and companies alike—through a wide range of cybercrimes. The Government respectfully submits that a significant jail term is necessary to deter O'Connor from continuing to victimize others from behind the computer screen.

The Government recognizes and has carefully considered the mitigating factors present in O'Connor's personal history and characteristics. O'Connor was young (about 20 or 21) when he committed the crimes in this case. He witnessed domestic violence and experienced verbal abuse and bullying while growing up. (PSR ¶¶ 164-65, 189). He was recently [redacted]. (PSR ¶¶ 185-86). Although O'Connor lived alone at the time of his arrest in this case, his mother was supporting him by providing for his basic needs, such as by ordering food for him. (PSR ¶ 174).

This Court can, and should, take all of these factors into account as it considers the appropriate sentence under Section 3553(a). However, the Government respectfully submits that these factors, taken either alone or together, do not excuse or justify O'Connor's criminal choices—his decisions, time and time again, to target, defraud, and traumatize others through cyber-attacks. [redacted]

But the crimes that O'Connor methodically perpetrated against his victims in this case show that he *is* dangerous. And O'Connor clearly knew right from wrong when he was committing these serious crimes. There is no dispute—and O'Connor admitted as much under oath during his plea—that, at the time that he committed his crimes, he knew that victimizing others through cybercrime was wrong and illegal. (Plea Tr. 25:13-18, Dkt. No. 11). Yet, O'Connor chose to do it anyway—time and time again. As this Court observed during O'Connor's arraignment, O'Connor's claimed dependence on his mother "didn't stop him from utilizing the internet" for criminal purposes. (Arraignment Tr. 13:22-23).[14] It was O'Connor, and O'Connor alone, who chose to defraud and abuse his many victims. There simply is no excuse for his crimes.

Finally, while mitigating factors of the kind cited by the defense may well call for a below-Guidelines sentence in other cases, this is a case in which the Guidelines do not capture the essence of the defendant's criminal conduct. For nearly 1.5 years, O'Connor deliberately targeted, defrauded, threatened, and extorted his victims. His criminal conduct not only caused financial losses, but it also inflicted significant emotional and psychological harm on his victims. This is a critical consideration for this Court as it determines the appropriate sentence for O'Connor, and yet it is not captured by the Guidelines at all. In particular, the Guidelines in no way capture O'Connor's crimes toward the individual victims in the NDCA Case, including Victim-3, a minor whom O'Connor abused and subjected to relentless swatting attacks. Balancing these considerations under Section 3553(a), the Government respectfully submits that a sentence of

[14] It is worth noting that O'Connor lived alone in Spain at the time of his arrest there on the charges in this case. (PSR ¶ 174). Although his mother reported visiting and assisting O'Connor (*id.*), it is clear that he is an individual who is capable of living independently and making his own decisions.

seven years' imprisonment, while it falls within the Guidelines range, is an appropriate and just sentence on the facts of this case.

3. The Need to Afford Adequate Deterrence and Promote Respect for the Law

One of the paramount factors that the Court must consider in imposing sentence under Section 3553(a) is the need for the sentence to "afford adequate deterrence to criminal conduct" and "promote respect for the law." 18 U.S.C. § 3553(a)(2)(A)-(B). As the Second Circuit has recently observed, "consideration of general deterrence is especially important" in white-collar cases. *Watts v. United States*, No. 21-2925, 2023 WL 2910634, at *4 (2d Cir. Apr. 12, 2023); *accord United States v. Martin*, 455 F.3d 1227, 1240 (11th Cir. 2006) (noting that legislative history of Section 3553(a) supports conclusion that "Congress viewed deterrence as particularly important in the area of white collar crime"); *United States v. Mueffelman*, 470 F.3d 33, 40 (1st Cir. 2006) (deterrence of white-collar crime is "of central concern to Congress"). "Because economic and fraud-based crimes are more rational, cool, and calculated than sudden crimes of passion or opportunity, these crimes are prime candidates for general deterrence." *Martin*, 455 F.3d at 1240. "Defendants in white collar crimes often calculate the financial gain and risk of loss, and white collar crime therefore can be affected and reduced with serious punishment." *Id.*

The sentence imposed upon O'Connor must send a strong message to the public that perpetrating fraud and computer crimes will not be treated leniently and will entail a significant period of incarceration. Such a message is particularly important at a time when hacking and other computer crimes have become an ever more prevalent and pernicious threat in our society. According to the FBI's 2021 Internet Crime Report, losses from internet-related crime have

increased five-fold from $1.4 billion in 2017 to $6.9 billion in 2021.[15] Using inexpensive and widely available hacking tools and techniques, cyber criminals can readily obtain access to and control over others' computers. With such unfettered access, cyber criminals can steal the victims' personal and financial information, spy on them, stalk them, or extort them. In addition, given the anonymity and worldwide reach of the Internet, and the proliferation of tools available to cyber criminals to mask their identities and conceal their crimes, it is often very difficult for law enforcement to detect and stop cybercrime and to identify, much less apprehend and prosecute, cyber criminals, many of whom, like O'Connor, are foreign actors. As a result, to afford general deterrence in the cybercrime context, courts must send a strong message to the public that lucrative and difficult-to-detect computer crimes will result in serious punishment if and when their perpetrators are caught. *See United States v. Zukerman*, 897 F.3d 423, 429 (2d Cir. 2018) ("Considerations of (general) deterrence argue for punishing more heavily those offenses that either are lucrative or are difficult to detect and punish, since both attributes go to increase the expected benefits of a crime and hence the punishment required to deter it.").

Moreover, computer crimes carry significant costs—financial, reputational, and emotional—for their victims and the public. These crimes undermine confidence in the electronic infrastructure used to facilitate everyday transactions and communications and increase the cost of cybersecurity for everyone. Moreover, many victims of cybercrimes lack effective tools to promptly detect network intrusions and data theft, leading to their targeting, victimization, and re-victimization. As can be seen from the facts of this case, cybercrime can also inflict significant emotional harm on its victims. To achieve the critical goal of general deterrence in the cybercrime

[15] *See* 2021 FBI Internet Crime Report at 7, *available at* https://www.ic3.gov/Media/PDF/AnnualReport/2021_IC3Report.pdf.

context, it is therefore imperative that those who would consider engaging in these forms of criminal conduct understand that the consequences will be serious if their crimes are uncovered and prosecuted.

II. The Court Should Award Restitution in Favor of O'Connor's Victims

A. Applicable Law

The Mandatory Victims Restitution Act ("MVRA") requires that a defendant convicted of specific crimes, including "an offense against property under this title . . . , including any offense committed by fraud or deceit," to "make restitution to the victim of the offense." 18 U.S.C. §§ 3663A(a)(1), (c)(1)(A)(ii). A "victim" is any "person directly and proximately harmed as a result of the commission of an offense," and, "in the case of an offense that involves as an element a scheme, conspiracy, or pattern of criminal activity, any person directly harmed by the defendant's criminal conduct in the course of the scheme, conspiracy, or pattern." 18 U.S.C. § 3663A(a)(2). "The court shall also order, if agreed to by the parties in a plea agreement, restitution to persons other than the victim of the offense." 18 U.S.C. § 3663A(a)(3). The expenses recoverable by victims as restitution include, among other things, "expenses incurred during participation in the investigation or prosecution of the offense or attendance at proceedings related to the offense." 18 U.S.C. § 3663A(b)(4).

"[T]he purpose of restitution is essentially compensatory: to restore a victim, to the extent money can do so, to the position he occupied before sustaining injury." *United States v. Boccagna*, 450 F.3d 107, 115 (2d Cir. 2006). The "primary and overarching" goal of the MVRA is "to make victims of crime whole, to fully compensate these victims for their losses and to restore these victims to their original state of well-being." *Id.*; *see also United States v. Calderon*, 944 F.3d 72, 94 (2d Cir. 2019) ("[R]estitution is designed to make the victim whole . . . and must therefore be

based only on the actual loss caused by the scheme."). It is "significant that the statute mandates that courts 'order restitution to each victim in the full amount of each victim's losses as determined by the court[.]'" *United States v. Quarashi*, 634 F.3d 699, 703 (2d Cir. 2011) (quoting 18 U.S.C. § 3664(f)(1)(A)).

Under the MVRA, "restitution may be imposed only for losses arising from the specific conduct that is the basis of the offense of conviction." *United States v. Goodrich*, 12 F.4th 219, 228 (2d Cir. 2021); *see also Hughey v. United States*, 495 U.S. 411, 413 (1990). In the context of a criminal conspiracy, restitution is not limited only to "losses caused by the actions of that defendant during the conspiracy, but also embraces losses flowing from the reasonably foreseeable actions of that defendant's co-conspirators." *Goodrich*, 12 F.4th at 228. The "MVRA requires that the 'offense' of conviction 'directly and proximately harmed' the victim entitled to restitution. Courts have interpreted this language to impose cause-in-fact and proximate cause requirements, respectively." *Id.* at 229. "Regarding cause in fact, the defendant's conduct must have been a necessary factor in bringing about the victim's harm." *Id.* Regarding proximate cause, the "basic question . . . is whether the harm alleged has a sufficiently close connection to the conduct, which we evaluate based on whether that harm was 'foreseeable' to a defendant." *Id.*

In the context of crimes resulting in damage or loss or destruction of property, compensable losses are measured by "(i) the greater of—(I) the value of the property on the date of the damage, loss, or destruction; or (II) the value of the property on the date of sentencing, less (ii) the value (as of the date the property is returned) of any part of the property that is returned." 18 U.S.C. § 3663A(b)(1)(B). When determining the appropriate amount of restitution, district courts must choose a valuation method that best accomplishes the purpose of the MVRA, namely to make the victim whole. *See Boccagna*, 450 F.3d at 115 ("[W]e construe 'value' as used in the MVRA to be

a flexible concept to be calculated by a district court by the measure that best serves Congress's statutory purpose.").

"Any dispute as to the proper amount or type of restitution shall be resolved by the court by the preponderance of the evidence." 18 U.S.C. § 3664(e). The "MVRA requires only a reasonable approximation of losses supported by a sound methodology." *United States v. Gushlak*, 728 F.3d 184, 196 (2d Cir. 2013). "[T]he preponderance standard must be applied in a practical, common-sense way. So long as the basis for reasonable approximation is at hand, difficulties in achieving exact measurements will not preclude a trial court from ordering restitution." *Id.*

B. Discussion

As part of his plea agreement, O'Connor agreed to make restitution in the amount of "at least" $794,000 to Company-1, as well as restitution in the total amount of $119,219.48 to SDNY Individual Victims-1 through -3, referred to in the plea agreement as "persons other than victims of the offenses charged in the SDNY Indictment." (PSR ¶ 40). The figure of $794,000 in the plea agreement reflects the value of the cryptocurrency stolen from Company-1 *as of the date of the theft* (May 1, 2019).

Following the entry of the plea agreement, Company-1, through counsel, has informed the Government and the Probation Office that it is seeking a total restitution award of approximately $1,980,483, comprising:

- The value of the Stolen Cryptocurrency *as of the date of O'Connor's sentencing* (June 23, 2023): estimated to be approximately $1,471,000;[16]

[16] None of the Stolen Cryptocurrency has been returned to Company-1 or its clients.

- The cost of Company-1's 2020 settlement with one of Company-1's clients whose cryptocurrency was stolen as part of the cyber intrusion, less the value of the client's stolen cryptocurrency as of the date of the settlement (to avoid double counting): $504,198;[17] and

- The cost of legal fees related to preparing for the restitution proceeding in this case: $5,285.

(PSR ¶ 90).[18]

Counsel for Company-1 is correct that where, as here, the value of the stolen property (cryptocurrency) as of the date of sentencing is greater than its value as of the date of the crime, the former is properly awarded as restitution to the victim. *See* 18 U.S.C. § 3663A(b)(1)(B); *Boccagna*, 450 F.3d at 114. The additional amounts requested by Company-1—namely, its legal fees related to preparing for the restitution proceeding in this case, as well as the balance of its settlement with its client stemming from the cyber intrusion committed by O'Connor and his co-conspirators (reflecting reputation costs and other harms experienced by the client in addition to the value of the stolen cryptocurrency)—are also properly recoverable as restitution, as these amounts were both directly and proximately caused by the criminal conduct of O'Connor and his co-conspirators and were reasonably foreseeable to O'Connor. *See United States v. Afriyie*, 27 F.4th 161, 174 (2d Cir. 2022) ("[T]he expenses a victim incurs while preparing for and

[17] According to Company-1's counsel, the amount of $504,198 represents compensation to Company-1's client for damages to reputation and other costs caused by O'Connor's theft of cryptocurrency from the victim and as a necessary part of retaining the business relationship with the client.

[18] Counsel for Company-1 has detailed these and others financial harms that Company-1 suffered as a result of O'Connor's crimes in the victim impact statement submitted to the Court, attached hereto as Exhibit A. Although the victim impact statement describes higher financial losses than that set forth above, counsel has subsequently clarified that Company-1 is seeking restitution only in the above-listed amounts (totaling approximately $1,980,483). However, Company-1, through counsel, requests that the Court consider the additional financial harms it has suffered, as well as the non-economic effects of O'Connor's crimes, as it determines the appropriate sentence pursuant to Section 3553(a).

participating in restitution proceedings are 'incurred during participation in the . . . prosecution of the offense or attendance at proceedings related to the offense' and so may be recovered to the extent the district court finds them necessary." (quoting 18 U.S.C. § 3663A(b)(4))); *cf. United States v. Glencore Int'l A.G.*, No. 22 CR. 297 (LGS), 2023 WL 2242469, at *6-7 (S.D.N.Y. Feb. 27, 2023) (awarding restitution for lost business in order to make the victim whole).

Because the value of the Stolen Cryptocurrency as of the date of O'Connor's sentencing cannot be determined with precision until the date of sentencing, the Government will provide a proposed restitution order to the Court as soon as practicable after sentencing (and in advance of the 90-day deadline, *see* 18 U.S. Code § 3664(d)(5)). The proposed restitution order will also set forth the additional amounts set forth above in favor of Company-1, the amounts agreed upon in the parties' plea agreement in favor of SDNY Individual Victims-1 through -3, and any amounts in favor of the victims in the NDCA Case.[19]

[19] The Court has previously entered a consent preliminary order of forfeiture against O'Connor. (Dkt. No. 10). The Government respectfully requests that the Court orally pronounce the forfeiture money judgment award ($794,012.64) during O'Connor's sentencing and include the consent preliminary order of forfeiture with the judgment in this case.

CONCLUSION

On the facts of this case, a sentence of seven years' imprisonment is appropriate and just. Such a sentence is necessary to reflect the seriousness of O'Connor's crimes, provide just punishment, afford general and specific deterrence, protect the public, and promote respect for the law.

Dated: New York, New York
June 19, 2023

Respectfully Submitted,

DAMIAN WILLIAMS
United States Attorney for the
Southern District of New York

By: /s/
Olga I. Zverovich
Assistant United States Attorney
(212) 637-2514

KENNETH A. POLITE, JR.
Assistant Attorney General
Criminal Division
U.S. Department of Justice

By: /s/
Adrienne L. Rose
Assistant Deputy Chief
(202) 532-4779

Cc: Defense Counsel
(Via ECF)